CLAIMS

1. A method for providing access to data stored in a repository forming part of a network, said access being requested from a node also forming part of said network, said method comprising:

receiving at an access control node user identification, user password and node identification data, said access control node interposed between said node and said repository;

said access control node transmitting over said network said user identification, user password and node identification requesting authentication for said access request;

said access control node receiving control signals responsive to said authentication request; and

responsive to said received control signals, selectively providing access to a subset of the functionality provided by said node.

2. The method of claim 1 wherein said selectively providing access to a subset of the functionality provided by said node comprises:

selectively providing electrical power to portions of said node.

3. The method of claim 2 wherein selectively providing electrical power to portions of said node provides for control of peripheral devices forming part of said node.

4. The method of claim 1 wherein said selectively providing access to a subset of the functionality provided by said node comprises:

selectively providing I/O signals to said node.

5. The method of claim 4 wherein selectively providing I/O signals to said node comprises allowing some I/O signals to be transmitted to said node while denying transmission of other I/O signals to said node.

6. The method of claim 1 wherein said user identification comprises a user identification token.

7. The method of claim 6 wherein said user identification token comprises data collected from at least one of: a magnetic card; a radio-frequency transmission or a biometrics scan.

8. A method for providing access to data stored in a repository forming part of a network, said access being requested from a node forming part of said network, said method comprising:

receiving user identification, user password and node identification data from an access control node associated with said node; and

transmitting control signals to said access control node, said control signals indicating limitations on the type of functionality to be provided to the user by said node, said user associated with said user identification and password.

9. The method of claim 8 further comprising:

generating said control signals, said control signals indicating:

if said user name and password data accurately correspond to an active user account, the type of access which is to be granted to said node; and

if said user name and password data do not accurately correspond to an active user account, a denial of access to said data in said repository.

10. The method of claim 9 wherein the type of access which is to be provided to said user comprise limitations on the data available for access by said user and limits on the use of

said data available for access, said limitations determined in view of said received user identification, user password and node identification data.

11. The method of claim 8 further comprising:

intercepting messages transmitted to said node from other parts of said network; and

transmitting to a security repository a log event corresponding to each activity described by said intercepted messages.

12. The method of claim 11 wherein said transmitting to a security repository an event log comprises:

analysing said intercepted messages; and

generating said event log responsive to said analysis.

13. The method of claim 12 wherein said analysing comprises capturing audit information from said intercepted messages and said generating said log event comprises formatting said captured audit information into an audit log record.

14. The method of 13 wherein said intercepted messages conform with at least one of the DICOM and HL7 data formats and wherein said audit log record comprises data in the extensible mark-up language.

15. The method of claim 8 further comprising:

intercepting messages transmitted from said node to a repository forming part of said network; and

transmitting to a security repository a log event corresponding to each activity described by said intercepted messages.

16. The method of claim 15 wherein said transmitting to a security repository an event log comprises:

analysing said intercepted messages; and

generating said event log responsive to said analysis.

17. The method of claim 16 wherein said analysing comprises capturing audit information from said intercepted messages and said generating said log event comprises formatting said captured audit information into an audit log record.

18. The method of claim 17 wherein said intercepted messages conform with at least one of the DICOM and HL7 data formats and wherein said audit log record comprises data in the extensible mark-up language.

19. The method of claim 15 further comprising:

if said user name and password data accurately correspond to an active user account, identifying the data and repositories to which access is to be granted; and

if said user name and password data accurately correspond to an active user account, allowing only those intercepted messages to proceed to said repository if access to said data in said repository has been granted.

20. The method of claim 19 further comprising, prior to allowing only those intercepted messages to proceed, analysing the content of said messages.

21. The method of claim 9 wherein said control signals further indicate:

if said node identification data does not correspond to a recognised node, denial of access by said node to said repository.

22. The method of claim 8 further comprising:

transmitting to a security repository a log event corresponding to each activity described by said intercepted messages.

23. The method of claim 8 further comprising:

responsive for a request for log event data, retrieving from said security repository log event data satisfying said request.

24. The method of claim 8 further comprising:

providing a means for configuring said user identification and password data for new and existing users.

25. The method of claim 24 wherein said means for configuring comprises at least one of:

defining roles to which users will associated;

for each role defined, identifying the data for which access is to be granted and the type of functionality at a node that is to be made available to a user associated with a role; and

associating users with at least one of said defined roles.

26. A device for providing control of a node, said node forming part of a network, said device comprising:

an input for receiving user identification, user password and node identification data, said device interposed between said node and the remainder of said network;

an output adapted to transmit over said network said user identification, user password and node identification and data requesting authentication of the user identification, user password and node identification and, responsive thereto, receive control signals responsive to said authentication request; and

a switching device for selectively providing access to a subset of the functionality provided by said node.

27. The device of claim 26 wherein said selectively providing access to a subset of the functionality provided by said node comprises selectively providing electrical power to portions of said node.

28. The device of claim 27 wherein selectively providing electrical power to portions of said node provides for control of peripheral devices forming part of said node.

29. The device of claim 26 wherein said selectively providing access to a subset of the functionality provided by said node comprises:

selectively providing I/O signals to said node.

30. The device of claim 29 wherein selectively providing video signals to said node comprises allowing some I/O signals to be transmitted to said node while denying transmission of other I/O signals to said node.

31. The device of claim 26 wherein said user identification comprises a user identification token.

32. The device of claim 27 wherein said user identification token comprises data collected from at least one of: a magnetic card; a radio-frequency transmission or a biometrics scan.

33. A computer readable media storing data and instructions, said data and instructions when executed by a general purpose computer adapt said computer to provide access to data stored in a repository forming part of a network, said access being requested from a node forming part of said network, said data and instructions adapting said general purpose computer to:

receive user identification, user password and node identification data from an access control node associated with said node; and

transmit control signals to said access control node, said control signals indicating limitations on the type of functionality to be provided to the user by said node, said user associated with said user identification and password.

34. The computer readable media of claim 32, wherein said data and instructions further adapting said general purpose computer to:

generate said control signals, said control signals indicating:

if said user name and password data accurately correspond to an active user account, the type of access which is to be granted to said node; and

if said user name and password data do not accurately correspond to an active user account, a denial of access to said data in said repository.

35. The computer readable media of claim 34 wherein the type of access to said user comprise limitations on the data available for access by said user and limits on the use of said data available for access, said limitations determined in view of said received user identification, user password and node identification data.

36. The computer readable media of claim 33 said data and instructions further adapting said general purpose computer to:

intercept messages transmitted to said node from other parts of said network; and

transmit to a security repository a log event corresponding to each activity described by said intercepted messages.

37. The computer readable media of claim 36 wherein said adaptation to transmit to a security repository an event log comprises adaptations to:

analyse said intercepted messages; and

generate said event log responsive to said analysis.

38. The computer readable media of claim 37 wherein said adaptation to analyse comprises capturing audit information from said intercepted messages and said adaptation to generate said log event comprises formatting said captured audit information into an audit log record.

39. The computer readable media of claim 33 said data and instructions further adapting said general purpose computer to:

intercept messages transmitted from said node to a repository forming part of said network; and

transmit to a security repository a log event corresponding to each activity described by said intercepted messages.

40. The computer readable media of claim 39 wherein said adaptation to transmit to a security repository an event log comprises an adaptation to:

analyse said intercepted messages; and

generate said event log responsive to said analysis.

41. The computer readable media of claim 40 wherein said adaptation to analyse comprises an adaptation to capture audit information from said intercepted messages and said adaptation to generate said log event comprises an adaptation to format said captured audit information into an audit log record.

42. The computer readable media of 41 wherein said intercepted messages conform with at least one of the DICOM and HL7 data formats and wherein said audit log record comprises data in the extensible mark-up language.

43. The computer readable media of claim 39 said data and instructions further adapting said general purpose computer to:

if said user name and password data accurately correspond to an active user account, identify the data and repositories to which access is to be granted; and

if said user name and password data accurately correspond to an active user account, allowing only those intercepted messages to proceed to said repository if access to said data in said repository has been granted.

44. The computer readable media of claim 43 said data and instructions further adapting said general purpose computer to, prior to allowing only those intercepted messages to proceed, analyse the content of said messages.

45. The computer readable media of claim 34 wherein said control signals further indicate:

if said node identification data does not correspond to a recognised node, denial of access by said node to said repository.

46. The computer readable media of claim 32 said data and instructions further adapting said general purpose computer to:

transmit to a security repository a log event corresponding to each activity described by said intercepted messages.

47. The computer readable media of claim 32 said data and instructions further adapting said general purpose computer to:

responsive for a request for log event data, retrieve from said security repository log event data satisfying said request.

48. The computer readable media of claim 32 said data and instructions further adapting said general purpose computer to:

provide a means for configuring said user identification and password data for new and existing users.

49. The computer readable media of claim 48 wherein said means for configuring comprises at least one of:

defining roles to which users will associated;

for each role defined, identifying the data for which access is to be granted and the type of functionality at a node that is to be made available to a user associated with a role; and

associating users with at least one of said defined roles.

50. A method for generating audit logs for a network, said network comprising a plurality of nodes interconnected by way of a communications network, said method comprising:

upon initial access by any user of a plurality of users, generating a login event record from user identification and password data received from an access control point from a plurality access control points, each of said plurality of access control points associated with one of said plurality of nodes;

intercepting all messages transmitted to or from each of said plurality of nodes; and

storing an audit log event in a repository for each activity identified in said intercepted messages.

51. The method of claim 50 further comprising:

analysing said intercepted messages so as to determine the activities represented by said intercepted messages.

52. The method of claim 51 wherein said analysing comprises:

identifying the format of the intercepted messages;

for each format identified, passing a subset of intercepted messages conforming to the format identified to a decoder for processing that format;

each decoder capturing activity and audit information from said subset of intercepted messages passed.

53. The method of claim 52 wherein the format of the intercepted messages conforms to at least one of: the DICOM and HL7 data formats.

54. The method of claim 51 further comprising:

prior to said storing, generating said audit log event for each identified activity in said intercepted messages.

55. The method of claim 54 wherein said generating comprises:

creating said audit log event for each identified activity in said intercepted messages from data captured during said analysing.

56. The method of claim 55 wherein said audit log events conform to the extensible mark-up language (XML).

57. The method of claim 51 wherein each audit log event comprises a digital signature.

58. A method for providing access to data for a plurality of users, said to data stored on a network, said network comprising a plurality of nodes, each of said plurality nodes associated with an access control node, each of said access control nodes interposed between its associated node and the network, said method comprising:

defining a plurality of roles to which users will associated;

for each role defined, identifying the data for which access is to be granted and the type of functionality at each of said plurality of nodes that is to be made available to a user associated with a role; and

associating each of said plurality of users with at least one of said defined roles.

59. The method of claim 58 further comprising:

for each attempted access to said data by a user at node, receiving user identification, password and node identification data;

if said user identification and password correspond to an active user account, generating a control signal indicating any limitations on the functionality of the node from which access has been attempted;

transmitting said control signal to the access control node associated with the node from which access has been attempted.

60. The method of claim 59 wherein said limitations on the functionality of the node are determined based on the capability of the node and the one or more roles which are associated with said active user account.

61. The method of claim 60 wherein said the capability of the node is determined by reference to repository of the capabilities of each of said plurality of nodes in the network in view of the node identification data received.